

GRC TOOLKIT

Self Assessment tool for conducting Risk Assessment based on COSO definitions

Relate each question to the Company's operational or financial procedures, relevant EU directive, Company Practice, Decision taken and Actions required

1. Control Environment

- Ethics:** Ethical environments are not successfully established and nurtured.
- Authorization:** Lines of authority, both spending authorization and operational executions) are not properly defined and consistently applied.
- Board Governance:** Board duties and obligations are not discharged in good faith or members are not possess adequate knowledge to interpret and act on the information provided.
- Business Continuity:** Business continuation plans (in the event of natural or manmade disaster) are not adequately planned, documented and tested.
- Fraud (Financial Misstatements):** Fraudulent activities related to financial reporting of company earnings, expenses, margins, and profits (etc.) are occurring and go undetected.
- Fraud (Operations):** Fraud and illegal acts are occur during the execution of day to day business operations and are go undetected.
- Physical Security:** Physical security of facilities, employees and the IT infrastructure is not effective or managed to an appropriate level.
- Personnel:** Procedures to attract, train and retain quality personnel (includes compensation & benefits) are not effective.

2. Risk Assessment

- Liquidity:** Cash forecasting is not effective to appropriately measure and manage cash needs and positions.
- Credit Ratings:** Credit/debt ratings are not appropriately managed to the company's best interest.
- Credit:** Creditworthiness of customers and maintenance of credit information and relationships with counterparties and suppliers are not adequately managed and maintained.
- Fuel Supply:** Necessary fuel supplies for native load and generation requirements (gas and electric) are not adequately planned, forecasted and obtained.
- Insurance:** Appropriate insurance coverage for various disciplines (e.g. workman's compensation, contractual exposure, officers D&O) are not adequately secured and managed.
- Strategic Focus:** Business strategies are not appropriately set and communicated including establishment and alignment of performance measures and incentive goals
- Budgeting – O&M:** Funds for day to day execution of operations are not being adequately planned, forecasted and budgeted.
- Budgeting -Capital:** Capital needs and requirements to run the utility are not adequately planned, forecasted and budgeted.
- Capacity – Generation/Transmission:** Capacity needs are not appropriately managed and forecasted.
- Legislation:** Legislative actions that are impact the utility are not adequately monitored and managed.
- Capacity – Pipeline:** Capacity needs are not appropriately managed and forecasted.

3. Control Activities

- ❑ **Meter Processes:** Processes around setting, installing, maintaining and testing meters are not effectively managed and executed.
- ❑ **Accounting/Financial Information:** Revenue, expenditures, assets and liabilities are not accurately, completely and timely recorded.
- ❑ **Asset Management:** Assets such as (IT, facilities, fleet and materials inventory) are not appropriately managed and controlled.
- ❑ **Billing:** Customer bills are not complete, accurate or properly aligned with regulatory requirements and stated billing rates and practices
- ❑ **Collections:** Amounts due from customers are not collected in a timely manner.
- ❑ **Contracting:** Contracts and agreements are not effectively negotiated, reviewed, and executed.
- ❑ **Contract Management:** Existing contracts are not effectively monitored, audited and measured.
- ❑ **Cost Recovery:** Costs are not recovered in rate base to obtain an adequate rate of return
- ❑ **Financial Reporting:** Consolidated financial statements and the compilation of information for SEC and investor reporting purposes are misstated, incomplete or untimely.
- ❑ **Generation Operations:** Operations are not operated in an effective, efficient, economical and safe manner.
- ❑ **Transmission Operations:** Operations are not operated in an effective, efficient, economical and safe manner.
- ❑ **Distribution Operations:** Operations are operated in an effective, efficient, economical and safe manner.
- ❑ **Health & Safety:** Adequate processes to protect and support employees and customer's health and safety are not consistently executed.
- ❑ **Tax:** Application of federal and state income, excise, property, sales and use tax laws and/or tax planning are not adequate to provide for the best tax situation for the company.

4. Information and Communications

- ❑ **IT Change Control:** Effective change control techniques for system changes are not adequately employed.
- ❑ **IT Infrastructure:** Current and future information requirements including hardware, networks, software are not adequately supported or established.
- ❑ **Communications – External:** Communication processes to customers, communities, regulatory bodies, shareholders, vendors and other external parties are not timely and effective.
- ❑ **Communications – Internal:** Communications to employees are not timely and effective and in the spirit of Aquila values (open, honest)
- ❑ **IT Access/Security:** System security and back up recovery are not adequately maintained to operate IT systems.
- ❑ **IT Systems Support:** An adequate level of IT Systems support for critical applications are not exist or appropriately maintained.
- ❑ **Records Management:** An adequate records management system does not exist and are not provide for adequate protection or security for records
- ❑ **Reputation:** Community, media and individual customer relationships are not appropriately maintained.

5. Information and Communications

- ❑ **Compliance – Regulatory:** Regulatory tariffs and rulings are not adequately monitored and applied to company's processes.
- ❑ **Compliance -Environmental:** Environmental laws and regulations are not complied with.
- ❑ **Compliance –Legal:** Various federal standards (e.g., EU directives, Sarbanes Oxley, applicable Tax Codes and/or local/federal laws and regulations) are not complied with.
- ❑ **Compliance – Internal Policies/Procedures:** Internal policies and procedures are not adequately documented, understood or appropriately complied with throughout the organization.